REMARKS

This amendment is in response to the Official Action mailed October 22, 2004.

In the present paper, claim 2 has been amended. Claims 1-11 are presented for the Examiner's consideration in view of the following remarks:

Objection to the Specification

The Examiner has objected to the Specification because it mentions "a cable modem or 'CM'" with respect to FIG. 1, but does not indicate the location of that element on FIG. 1. Applicant has amended paragraph [0004] of the specification to remove the reference to FIG. 1, and submits that the objected-to informality is now corrected.

The Present Application

The present application is directed to a system and method for communication between a telephone and the public switched telephone network including transport of packets over cable television network facilities. Such systems typically include an Internet Protocol Digital Terminal ("IPDT") connecting telephony signals in the HFC network to the public switched telephone network (present specification at [0006]). Such systems may also include a plurality of Cable Modem Termination System/Edge Routers ("CMTS/ERs") located at cable head ends (spec. at [0004]). A drawback of prior art systems is the necessity of the IPDT, upon receipt of a call intended for cable telephony customer, to determine which CMTS/ER services that customer so that DQoS call setup signaling messages can be sent to the proper CMTS/ER.

The inventors have discovered a technique whereby that DQoS signaling message is encrypted and encapsulated in a Create Connection ("CRCX") signaling message sent to a Broadband Telephony Interface ("BTI"), which then forwards the encrypted DQoS signaling message to the proper CMTS/ER.

The system and method of the invention allow the call to be set up without the necessity of the IPDT determining which CMTS/ER services the customer, but also without trusting the BTI with that information.

In one exemplary embodiment claimed in independent claim 1, a method of Quality of Service Signaling in a system for cable telephony using one or more packet data networks includes the steps of (a) encrypting, at an Internet Protocol Digital Terminal, a Dynamic Quality of Service signaling message; and (b) transmitting a signaling message including said encrypted Dynamic Quality of Service signaling message to a Broadband Telephony Interface.

The Examiner has rejected claim 1 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,483,912 to Kalmanek, Jr. et al. (Kalmanek); has rejected claim 2 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,182,104 to Chapman ("Chapman") in view of Kalmanek; has rejected claims 3-5 and 9-11 under 35 U.S.C. § 103(a) as unpatentable over Kalmanek in view of Chapman; and has rejected claims 3-5 and 9-11 under 35 U.S.C. § 103(a) as unpatentable over Kalmanek in view of Chapman and further in view of U.S. Patent No. 6,028,933 to Heer ("Heer") .

The Kalmanek *Patent*

Kalmanek discloses a system for allocating network resources based on an authorized quality of service. FIG. 1 of that reference shows a telephone network gateway 130 connecting a telephone network 135 to a communication network 100. Network edge devices 120, 121 connect the communication network 100 to access networks 150, 151. Telephony interface units (TIUs) 170, 171 provide gateways between telephones 190, 191 and access networks 150, 151.

Gate controllers 110, 111 have access to authentication databases and customer profile information on database storage 140, 141. Kalmanek teaches encrypting state information passed from the gate controllers to the TIUs.

The Chapman *Patent*

Chapman discloses a technique for increasing effective bandwidth in a packet-based system by suppressing packet headers that are repetitive from packet to packet. The system is described in connection with a cable system extending between the cable modem (CM) and the cable modem termination system (CMTS). Chapman discusses the use of the Baseline Privacy Interface (BPI) standard of DOCSIS within the cable network between the CMs and the CMTS.

Discussion

Claim 1 Not Anticipated by Kalmanek

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131

(quoting Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

Applicants submit that each of the elements of claim 1 is not taught by Kalmanek, and that claim 1 is therefore patentable over that reference. Specifically, Kalmanek (1) does not teach encrypting at an Internet Protocol Digital Terminal, (2) does not teach transmitting a signaling message, and (3) does not teach a signaling message including an encrypted DQoS signaling message.

As to "encrypting, at an Internet Protocol Digital Terminal," the Examiner is asserting that the gate controller (e.g., gate controller 110) of FIG. 1 is an Internet Protocol Digital Terminal as that term is defined in the present specification:

> As explained on submitted disclosure on page 2, ref. Num [0005], lines 12-15, "an Internet Protocol Digital Terminal" is a device that is connected to the IP network to send signals to and receive signals from a "CMTS/ER". The office interpreted the "Gate Controller" which is shown on figure 1 as an Internet Protocol Digital Terminal" since it is a device that is connected to IP network which is shown on figure 1, ref. Num "100" and send signals to and receive signal from a "CMTS/ER".

Office Action mailed 10/22/2004, at 3. The present specification, however, requires that the IPDT be connected to <u>both</u> the IP network <u>and</u> to a local telephone company's local digital switch:

> In order to connect telephony signals in the HFC network to the public switched telephone network, a device that may be referred to as an "Internet Protocol Digital Terminal" or "IPDT" may be connected to the IP network (to send signals to and receive signals

> from a CMTS/ER) and to a telephone company's Local Digital Switch (or "LDS"), a local Class5 switch.

Specification at [0006] (emphasis added).

Because the gate controller 110 of Kalmanek is not connected to a local telephone company's Local Digital Switch, that element cannot be considered an IPDT, as that term is defined in the present specification.

As to the claim 1 requirement that a DQoS signaling message be encrypted and included in a transmitted signaling message, Applicants further assert that Kalmanek does not teach encrypting a DQoS signaling message. Instead, "state information" is encrypted before being sent to the TIUs (Kalmanek, col. 6, lines 21-27). Kalmanek does not teach or suggest that the "state information" is DQoS signaling information.

Applicants further submit that the message that is transmitted in Kalmanek is not a "signaling message including said encrypted DQoS signaling message," as required by claim 1. Instead, the encrypted state information in Kalmanek is simply transmitted to the TIUs and is not included in any signaling message.

In the exemplary embodiment disclosed in the present specification, the encrypted DQoS signaling message is included in the NCS message (CRCX or DLCX) that is sent by the IPDT to the BTI telling the BTI to set up a voice connection between the BTI and the IPDT (see specification at [0024] – [0025]). By including the encrypted signaling message in that signaling message, no additional messaging burden is added by the invention. In contrast, the encrypted state information of Kalmanek is simply passed from the gate controllers to the TUIs.

For each of the above reasons, Applicants submit that claim 1 is novel and non-obvious over the Kalmanek reference.

Claim 2 Not Obvious over Chapman in View of Kalmanek

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. M.P.E.P. § 2143.03 (*citing In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)).

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972).

Claim 2 has been amended to make clear that that the signaling message received from the Broadband Telephony Interface includes an encrypted Dynamic Quality of Service signaling message encrypted by an Internet Protocol Digital Terminal.

The Examiner has pointed to a passage of Chapman at col. 4, lines 45-52 as teaching the receipt, at a CMTS, of a signaling message including an encrypted DQoS signaling message. That passage of Chapman, in fact, describes the well-known baseline privacy encryption (BPI) of the DOCSIS standard. That encryption is used within a cable network; i.e., between a cable modem and a cable head end. In terms of the architecture of the present invention, BPI encryption might be used between the BTI and the CMTS/ER. Traffic upstream of the CMTS, including traffic between the CMTS and the IPDT, is not encrypted using BPI because the IPDT is outside the cable system. (see attached appendix entitled Cisco uBR7200 Series Software Configuration Guide, Chapter 4, at p. 3, "CAUTION" paragraph).

The BTI encryption of Chapman therefore cannot be performed by an IPDT, as required by claim 2. The IPDT is outside the cable network, and does not use DOCSIS or the BTI encryption standard of DOCSIS. Applicants therefore assert that Chapman does not teach the receiving step of claim 2, as amended.

Applicants further contend that neither Kalmanek nor Chapman teaches "a signaling message including an encrypted Dynamic Quality of Service signaling message" as required by claim 2. As noted above, Kalmanek does not teach including an encrypted DQoS signaling message in a signaling message. Similarly, Chapman does not teach including an encrypted message in a message, but instead teaches, at most, encrypting voice packets according to DOCSIS BPI standard.

Applicants respectfully assert that, for the reasons stated below, the Examiner has not established a *prima facie* case of obviousness because the combination of Chapman in view of Kalmanek does not teach or suggest several claim limitations.

Claims 3-8 Not Obvious over Kalmanek in View of Chapman

For the reasons set forth above with respect to claim 1, Applicants initially submit that the "Gate Controllers" of Kalmanek cannot be considered the IPDT of claims 3 and 9 because the present specification requires that the IPDT be connected to the IP network and to a local telephone company's Local Digital Switch. Furthermore, for the reasons set forth above, Applicants assert that Kalmanek does not teach encrypting a DQoS signaling message, but instead teaches, at most, encrypting "state information." Additionally, neither Kalmanek nor Chapman teaches "a signaling message including an encrypted Dynamic Quality of Service signaling message" as discussed above with respect to claims 1 and 2.

Claim 3 further requires, in part:

(a) encrypting a DQoS message at the IPDT;

(b) transmitting a signaling message including said encrypted DQoS message from the IPDT to a BTI; and

(c) transmitting a signaling message including said encrypted DQoS message from the BTI to a CMTS.

Thus, the same DQoS message that is encrypted by the IPDT is transmitted from the IPDT to the BTI, and from the BTI to the CMTS. Applicants respectfully assert that no combination of references cited by the Examiner teaches that sequence of events.

The examiner states that, as taught by Chapman, the packet included in the request to change access by the "CM" cable modem "includes the quality of service message [and] is encrypted as explained on column 4, lines 45-50." The packets described in that passage of Chapman, however, are BPI encrypted packets that, by definition, are within the cable modem network, as discussed above. A BPI encrypted packet therefore cannot be encrypted at the IPDT, as required by claim 3.

Furthermore, no message in Chapman or in Kalmanek is encrypted at the IPDT, transmitted to the BTI, and then transmitted to the CMTS, as required by claim 3. Chapman discloses, at most, sending BPI encrypted packets between the CM and the CMTS . Kalmanek discloses sending encrypted information to the TIUs.

For each of the above reasons, Applicants assert that independent claim 3 is patentable over Kalmanek in view of Chapman, and further submit that claims 3-8, which depend from claim 3, are patentable for at least the same reasons.

Claims 9-11 Not Obvious over Kalmanek in View of Chapman

For the reasons set forth above with respect to claim 3-8, Applicants submit that the limitations of claims 9-11 are not taught or suggested by the references cited by the Examiner, alone or in combination.

Conclusion

Applicants therefore respectfully assert that all the claims in the case are now in condition for allowance, and earnestly request that the Examiner issue a Notice of Allowance.

Should the Examiner have any questions regarding the present case, the Examiner should not hesitate in contacting the undersigned at the number provided below.

Respectfully submitted,

By_______________

Robert T. Canavan
Reg. No. 37,592
Telephone: 908-707-1568

Canavan & Monka LLC
250 State Route 28, Suite 207
Bridgewater, NJ 08807

Date: 6/28/2005

Chapter 4: Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series

Table Of Contents

Download this chapter
Chapter 4: Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series
Download the complete book
Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide (PDF - 3 MB)

GIVE US FEEDBACK

Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series

~~This chapter describes the DOCSIS 1.0 Baseline Privacy Interface (BPI),~~ guidelines for configuring DOCSIS BPI on the Cisco uBR7200 series, and features of DOCSIS 1.1 Baseline Privacy Interface Plus (BPI+). This chapter contains the following sections:

Section	Description
"Baseline Privacy Interface Overview" section	Provides a description of DOCSIS 1.0 BPI, BPI key management, CM cummunication with the BPI, and illustrations.
"Enabling DOCSIS BPI" section	Provides guidelines for enabling DOCSIS 1.0 BPI on the Cisco uBR7200 series.
"DOCSIS 1.1 Baseline Privacy Interface Plus Overview" section	Provides an overview of the features in DOCSIS 1.1 BPI+.

Baseline Privacy Interface Overview

Baseline Privacy Interface (BPI) is defined as a set of extended services within the DOCSIS MAC sublayer. BPI gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and CM.

Note Encryption/decryption is subject to export licensing controls.

The level of data privacy is roughly equivalent to that provided by dedicated line network access services such as analog modems or digital subscriber lines (DSL). BPI provides basic protection of service, ensuring that a CM, uniquely identified by its MAC address, can obtain keying material for services only it is authorized to access.

Note Because DOCSIS 1.0 BPI does not authenticate CMs, it does not protect against users employing cloned CMs masquerading as authorized CMs. Specific Cisco IOS releases provide protection against spoofing, and

provide supporting commands that can be used to configure source IP filtering on RF subnets to prevent a user from using a source IP address that is not valid for the connected IP subnet.

BPI extends the definition of the MAC sublayer's SID. The *DOCSIS RF Interface Specification* (viewable at http://www.cablemodem.com/specifications.html) defines a SID as a mapping between CMTS and CM to allocate upstream bandwidth and class of service management. When BPI is activated, the SID also identifies a particular security association and has upstream and downstream significance. When BPI is operational, downstream multicast traffic flow that typically does not have a SID associated with it, now has a SID. The Privacy Extended Header Element includes the SID associated with the MAC Packet Data Physical Data Unit (PDU). The SID along with other components of the extended header element identifies to a CM the keying material required to decrypt the MAC PDU's packet data field.

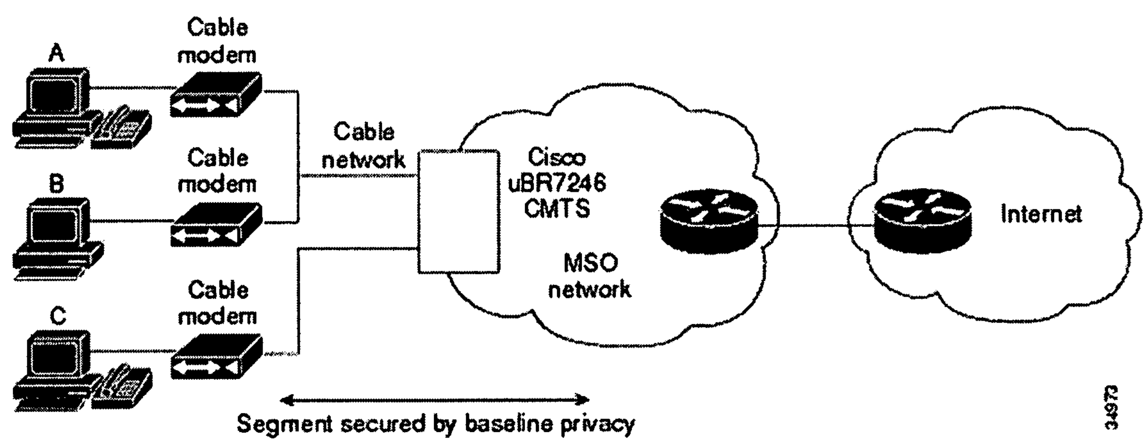
BPI's key management protocol runs between the CMTS and the CM. CMs use the protocol to obtain authorization and traffic keying material relevant to a particular SID from the CMTS and to support periodic reauthorization and key refresh.

The key management protocol uses RSA—a public key encryption algorithm—and the electronic codebook (ECB) mode of DES to secure key exchanges between the CMTS and a CM. Privacy is in the form of 56-bit (the default) or 40-bit encryption between the CMTS and CM. Since BPI is part of DOCSIS, all DOCSIS-certified CMs and qualified CMTS are fully interoperable. Figure 4-1shows a BPI architecture.

Note CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment.

A SID's keying material has a limited life span. When the CMTS delivers SID keying material to a CM, it also provides the CM with the lifetime value.

Figure 4-1 BPI Network Example



BPI Key Management

BPI initialization begins with the CM sending the CMTS an authorization request, containing data identifying:

- CM—48-bit IEEE MAC address
- CM's RSA public key
- List of zero or more assigned unicast SIDs that have been configured to run BPI

At that time, BPI provides basic protection against theft of service by ensuring the CM, identified by its MAC

address, can obtain keying materials only it is authorized to access. The CMTS replies with a list of SIDs on which to run BPI. The reply also includes an authorization key from which the CM and CMTS derive the keys needed to secure a CM's subsequent requests for additional encryption keys. After obtaining the traffic encryption key, the CMs begin to transmit encrypted data.

Differentiating Traffic Streams

BPI only encrypts data on the cable network and only encrypts the user data itself, not cable MAC headers. BPI also does not encrypt MAC management messages. After BPI is enabled, however, and encryption has been negotiated for a given SID, all user data sent via that SID is encrypted. BPI differentiates traffic based on SID alone.

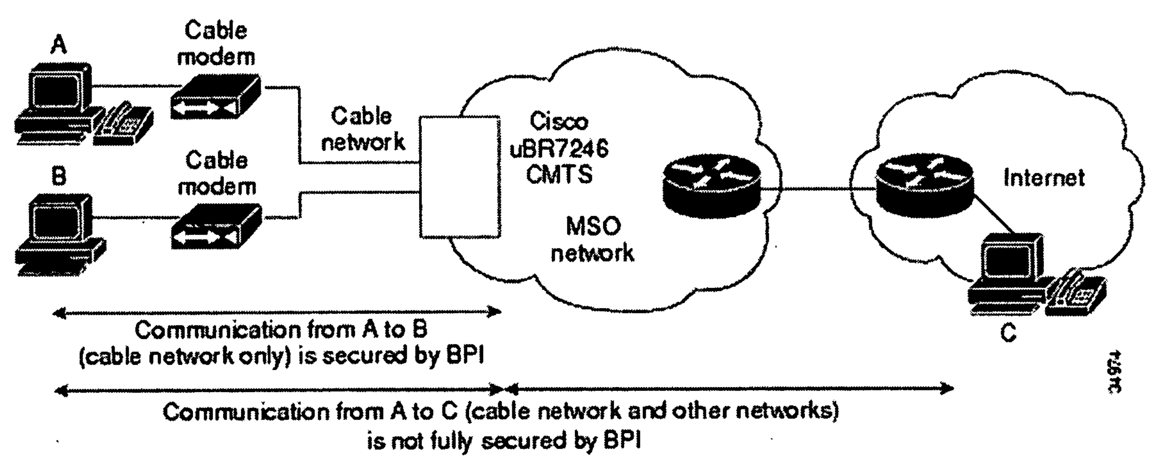
CM Communication with BPI

Figure 4-2 illustrates BPI communications. When user A sends packets to user B, the CM encrypts those packets using special keys specific to user's A CM. Packets are then transmitted to the CMTS where they are decrypted.

If user B is attached to the cable TV network, the CMTS then re-encrypts the information using a key specific to user B and the encrypted data is passed to user B's CM where it is decrypted and sent to user B. In this manner, an unauthorized user is not able to see unencrypted traffic between user A and user B.

Caution Since BPI occurs only on the cable TV network, however, all traffic going upstream will be decrypted as it passes the CMTS. If user A is attempting to communicate with someone beyond the cable network—user C—all traffic beyond the CMTS will not be encrypted.

Figure 4-2 BPI Encrypted Data on the Cable TV network



Enabling DOCSIS BPI

To enable BPI, choose software images at both the CMTS and CM that support the mode of operation. For the Cisco uBR7200 series software, choose an image with "k1" in its file name or BPI in the feature set description. For Cisco uBR924 cable access routers, all CM images from Cisco IOS Release 12.0(5)T1 or later support this by default. For earlier Cisco IOS release cable modem images, choose an image with "k1" in its file name or BPI in the feature set description.

Note For the CMTS, BPI is enabled by default when you select an image that supports BPI. For CMs, enable BPI via the DOCSIS configuration file using one of the provisioning tools identified in the "DOCSIS 1.0 Support" section on page 1-45.

When baseline privacy is enabled, the Cisco uBR7200 series generates Traffic Encryption Keys (TEKs) for each applicable SID; 56-bit encryption/decryption is the default for Cisco uBR7200 series equipment.

The router uses the keys to encrypt downstream data and decrypt upstream traffic from two-way cable interfaces. The Cisco uBR7200 series router generates keys for unicast, broadcast, and multicast operation as appropriate. Keys are refreshed periodically and have a default lifetime of 12 hours.

DOCSIS 1.1 Baseline Privacy Interface Plus Overview

DOCSIS 1.0 included a BPI to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- Digital certificates provide secure user identification and authentication.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Multicast support.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Note BPI+ is described in the *Baseline Privacy Interface Plus Specification* (SP-BPI+-I07-010829), available from CableLabs (http://www.cablelabs.com).

If you want to be contacted about your feedback, please enter your first and last names in the Name field and your email address in the E-Mail field.

Name

Email

Submit